

(19)



Europäisches Patentamt

European Patent Office

Office européen des brevets



(11)

EP 0 729 120 A2

(12)

## EUROPEAN PATENT APPLICATION

(43) Date of publication:

28.08.1996 Bulletin 1996/35

(51) Int. Cl.<sup>6</sup>: G07D 7/00, G07F 7/12

(21) Application number: 96102382.7

(22) Date of filing: 16.02.1996

(84) Designated Contracting States:  
DE FR GB

(30) Priority: 23.02.1995 US 392713

(71) Applicant: EASTMAN KODAK COMPANY  
Rochester, New York 14650-2201 (US)

(72) Inventors:

- Ray, Lawrence A.,  
c/o Eastman Kodak Company  
Rochester, New York 14650-2201 (US)

• Ellison, Richard N.,

c/o Eastman Kodak Company  
Rochester, New York 14650-2201 (US)

(74) Representative: Wagner, Karl H., Dipl.-Ing.  
WAGNER & GEYER  
Patentanwälte  
Gewürzmühlstrasse 5  
80538 München (DE)

## (54) Method and apparatus for image based validations of printed documents

(57) Multiple validations of printed documents incorporating image information and authorizing data on a printed document assist in the printed document validation process. This technique requires the authorized document holder to have an image identification accompany the application or production of the document. Image information is converted to a storable image that is used in one of a plurality of validating schemes that assures that the presenter of the printed document is not a substitute. Such schemes included visual comparison of the printed document presenter and extracted image information and validation that the data has not been altered. Non-reversible encryption of the data, as it is read from the document at the document presentation site is used to formulate encoded authorization data that is then compared against like encoded authorized document holder data stored at a centrally located data base.

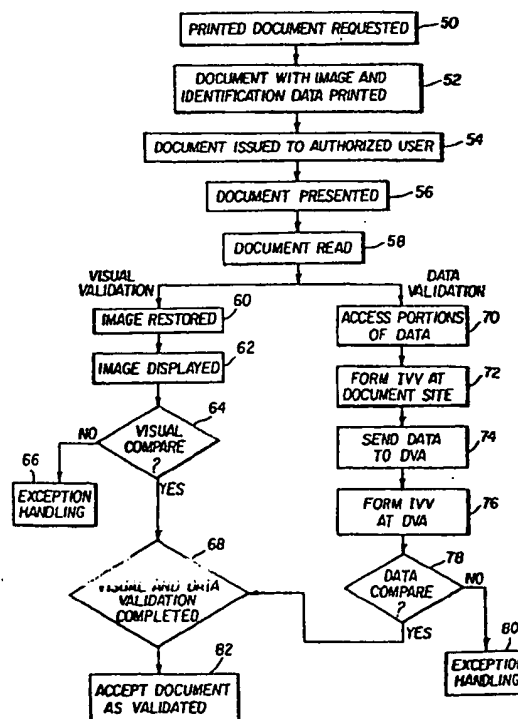


FIG. 4

document identification data and at least portions of the encoded data from said first processor, and accessing the image data associated with said printed document from said storage means, and for said second processor means to process said associated image data and portions of received data to form second processor encoded data, and comparing portions of received encoded data with said second processor encoded data to provide a validation signal when a correspondence is detected.

The present invention is a means of printing image information onto a printed document and using that information to assist in the validation process. The present invention consists of a plurality of printed documents each having data recorded thereon representing the image of at least one authorized user and document identification data. When the document is read at a document presentation site (e.g., the point of sale), the image is displayed and both the image data and document identification data are encoded by a non-reversible encryption algorithm. This information is then compared with similarly processed information stored at a remote site. If a correspondence is detected, a validation signal is transmitted from the remote site to the document presentation site.

The above and other objects of the present invention will become more apparent when taken in conjunction with the following description and drawings wherein identical reference numerals have been used, where possible, to designate identical elements that are common to the figures.

#### Advantageous Effects Of the Invention

The present invention has the following advantages: information concerning the validity of the document is doubly validated, at the document presentation site and at a remote, trusted site. Moreover, for the document to be validated, the same image information would have to be held by both the DVA and the printed document. The algorithm to validate the document would be modified by a document tampering, then the information used by the IVV algorithm would be different than the data available to the DVA and the IVV algorithm would produce a different result, invalidating the document. Moreover, since the algorithm selected randomly for each validation requester, attempting to circumvent the algorithm by clever re-encoding would also be thwarted, making fraudulent documents harder to produce. Also, knowledge that bearers of fraudulent documents would have their images captured will also be a deterrent, much like video cameras in banks.

Unlike other forms of printed document verification, the means of verification is largely transparent to the printed document holder. The method is non-intrusive and consumer friendly. There is also only a limited amount of printed space on the document needed to implement the present invention.

In the case of documents being checks, the cost of this would be recovered by the reduction of fraudulent purchases being made upon checks. Since this cost is borne by the merchant, the savings that result immediately improve the profitability of the merchant or the merchant can reduce prices to the customer.

The cost of producing documents in order to have the visual validation will only increase for the processing of the authorized document holder's image. In the case of checking, the printing of the check should be identical, as the image information is encoded as a two-dimensional bar code and can be printed with resolutions as coarse as 240 dots per inch.

Another advantage is that the authorized document holder will not be required to carry any additional information, such as a PIN number to corroborate the validity of the check or have a secondary identification, such as a driver's license. In the case where the document is a check, this will make the acceptance of the checks easier, as the validation comes with no significant inconvenience to the consumer.

The equipment necessary to perform this validation will not be significantly different that which is currently in place. In the case of checks, a check reader and a connection to a check validation agency is required. This is very similar to current practices though without the advantage of the secondary validation.

#### Brief Description of the Drawings

Fig. 1 is a printed document, in check form, containing readable data representing the image of the authorized user and document identification;

Fig. 2 is a block diagram illustrating the arrangement of the apparatus for performing the method of the present invention;

Fig. 3 is a block diagram illustrating a selection process for non-reversible encryption algorithms; and

Fig. 4 is a flow chart of the method of operation for the present invention.

#### Detailed Description of The Invention

Referring to Fig. 1, a sample printed document 10 is shown in the form of a standard bank check. Printed on the front of the check is a bar code 12. The bar code 12 represents information with a structured sequence of lines in a two-dimensional pattern, such as the PDF417 Code of Symbol Technologies of Bohemia, New York. The bar code 12 contains image data 20 relating to an image of an authorized document holder. The image data 20 may be in compressed form. The bar code 12 may also contain document identification data 18 for distinguishing the document from other documents issued to the same authorized user. The document identification data 18 may be the check sequence number. Although the bar code 12 is shown in the upper right hand corner of the check 10 it is obvious that other

In the case where a document has been damaged beyond recovery, of the data by means such as error correcting codes, then a back-up method is for the document validation requester to manually key the document identification data and to request the image data be sent from the DVA. An alternative image data format may be preferred if coded data interception is possible. Moreover, the DVA will be alerted to either a document presenter with a damaged document, or a document being used for fraudulent purposes.

Of course, the previous two methods can be used in combination to further insure the printed document has not been tampered.

The image data and/or information extracted from that image data is encoded and printed onto the document by means of a two-dimensional bar code such as the PDF417 by Symbol Technologies. This information can be used by the validation requester at the document presentation site to recover, for display, a picture of the document holder on a display device as a quick visual means for the validation requester to verify the validity of the document. In addition, as part of a validation procedure, each validation requester has, or is sent, an identification code which selects the algorithm to be accessed by the processor 26, which algorithm is then applied to the image data encoded on the document in order to generate an image-validation-value (IVV). This code may also be responsive to other information specific to the circumstances of the document presentation such as the date and time of the presentation.

Referring to Fig. 4, a flow chart of the method of operation of the present invention is illustrated. In block 50, the document holder requests the issuance of a printed document 20 and provides information for the printed document comprised of at least image information. The document with the image information and the assigned document identification data 18 is printed in block 52. Printed documents are issued to the authorized document holder in block 54. In the next step, block 56, the document holder presents the document at the document presentation site. The document is read in block 58. Two paths follow from block 58, a visual validation path and a data validation path. These processes occur in parallel and rejoin at block 68.

The visual validation path proceeds from block 58 to block 60 where the image data is processed into digital image data by possible decompression. Next, in block 62, the image data is displayed on a display device and viewed. In block 64, the operator compares the image of the authorized document holder now on the display with the document presenter. If the operator determines that the image of the authorized document holder fails to correspond to the appearance of the document presenter, then an exception process, block 66, is initiated. If the operator determines there exists a reasonable correspondence, then the visual validation path is completed and joins with the end of the data validation path at block 68.

The data validation path begins at block 70 with the extraction of portions of the read data from the local data storage 24. In block 72, the processor 26 encodes the data as described above to produce an IVV. This IVV and at least the document identification data is sent in block 74 to the processor 34 at the document validation authority. In block 76 another IVV is generated from the document identification data received and the retrieved image data of the authorized user from the data storage device 36. The two IVV's are compared in block 78. If the values do not match, in block 80 an exception handling process is initiated. For example, an exception handling process may consist of sending a non-validation signal to processor 26 at the document presentation site. Another example is for processor 34 to request processor 26 to transmit the image data to processor 34. If the comparison in block 78 yields a match, then a validation signal is sent to processor 26 at the document presentation site as shown in block 68. This terminates the data validation path. The path now rejoins with the visual validation path in block 68.

Block 68 waits for the successful completion of both the visual and data validations. When both validation signals are positive, the document is accepted and confirmed as having been presented by the authorized document presenter in block 82.

According to its broadest aspect, the invention relates to a printed document validation system comprising:

- a plurality of printed documents each having data recorded thereon representing the image of at least one authorized user and document identification data;
- reader means for reading the data recorded on said printed document; and
- algorithm means for providing a non-reversible encryption algorithm for encoding portions of the data.

It should be noted that the objects and advantages of the invention may be attained by means of any compatible combination(s) particularly pointed out in the items of the following summary of invention and the appended claims.

#### SUMMARY OF INVENTION

1. A printed document validation system comprising:

- a plurality of printed documents each having data recorded thereon representing the image of at least one authorized user and document identification data;

- reader means for reading the data recorded on said printed document;

- algorithm means for providing a non-reversible encryption algorithm for encoding portions of the data;

- a first processor means for encoding the data read from said printed document with the provided non-reversible encryption algorithm;

- means for displaying the image representing

said data to produce a document validation value; and

b. second processor means located at said document validation agency for producing a document validation value generated from applying said non-reversible encryption algorithm to data stored at said document validation agency.

9. The printed document validation system, wherein said non-reversible encryption algorithm is selected from a plurality of non-reversible encryption algorithms and further comprising means for transmitting a validation requester identification code identifying a selected non-reversible encryption algorithm from said document presentation site to said document validation agency.

10. The printed document validation system, further comprising means for transmitting said document validation value, said validation requester identification code and a printed document number from said document presentation site to said document validation agency.

#### Parts List:

10	Printed document
12	Bar code
14	Document Sequence Number
16	MICR line
18	Document identification data
20	Image data
22	Printed document reader
24	Local data storage
26	Document site processor
28	Digital image
30	Visual display device
32	Document site algorithm table
34	DVA processor
36	DVA data storage
38	DVA algorithm table
40	Algorithm switch
42	Non-reversible encryption algorithm
50	Printed document requested
52	Document printed
54	Document issued
56	Document presented
58	Document read
60	Image restored
62	Image displayed
64	Visual compare
66	Exception handling
68	Validations complete
70	Access data
72	Form IVV
74	Send data
76	Form IVV
78	Data compare

80 Exception handling

82 Accept document

#### Claims

1. A printed document validation system comprising:
  - a plurality of printed documents each having data recorded thereon representing the image of at least one authorized user and document identification data;
  - reader means for reading the data recorded on said printed document;
  - algorithm means for providing a non-reversible encryption algorithm for encoding portions of the data;
  - a first processor means for encoding the data read from said printed document with the provided non-reversible encryption algorithm;
  - means for displaying the image representing the authorized user;
  - a storage means having stored therein data corresponding to the image data recorded on said printed document;
  - and a second processor means for receiving the document identification data and at least portions of the encoded data from said first processor, and accessing the image data associated with said printed document from said storage means, and for said second processor means to process said associated image data and portions of received data to form second processor encoded data, and comparing portions of received encoded data with said second processor encoded data to provide a validation signal when a correspondence is detected.
2. A printed document validation system comprising:
  - a plurality of printed documents each having data recorded thereon representing the image of at least one authorized user, document identification data, and authorizing data;
  - reader means for reading the data recorded on said printed documents;
  - first algorithm means for providing a non-reversible encryption algorithm for encoding portions of the data;
  - a first processor means for encoding the data read from said printed document with the provided non-reversible encryption algorithm;
  - means for displaying the image representing the authorized user;
  - a second processor means for receiving the document identification data and portions of the encoded data from said first processor;
  - a storage means having stored therein data corresponding to the authorizing data recorded on said printed document; and
  - second algorithm means for providing a non-reversible encryption algorithm for encoding por-

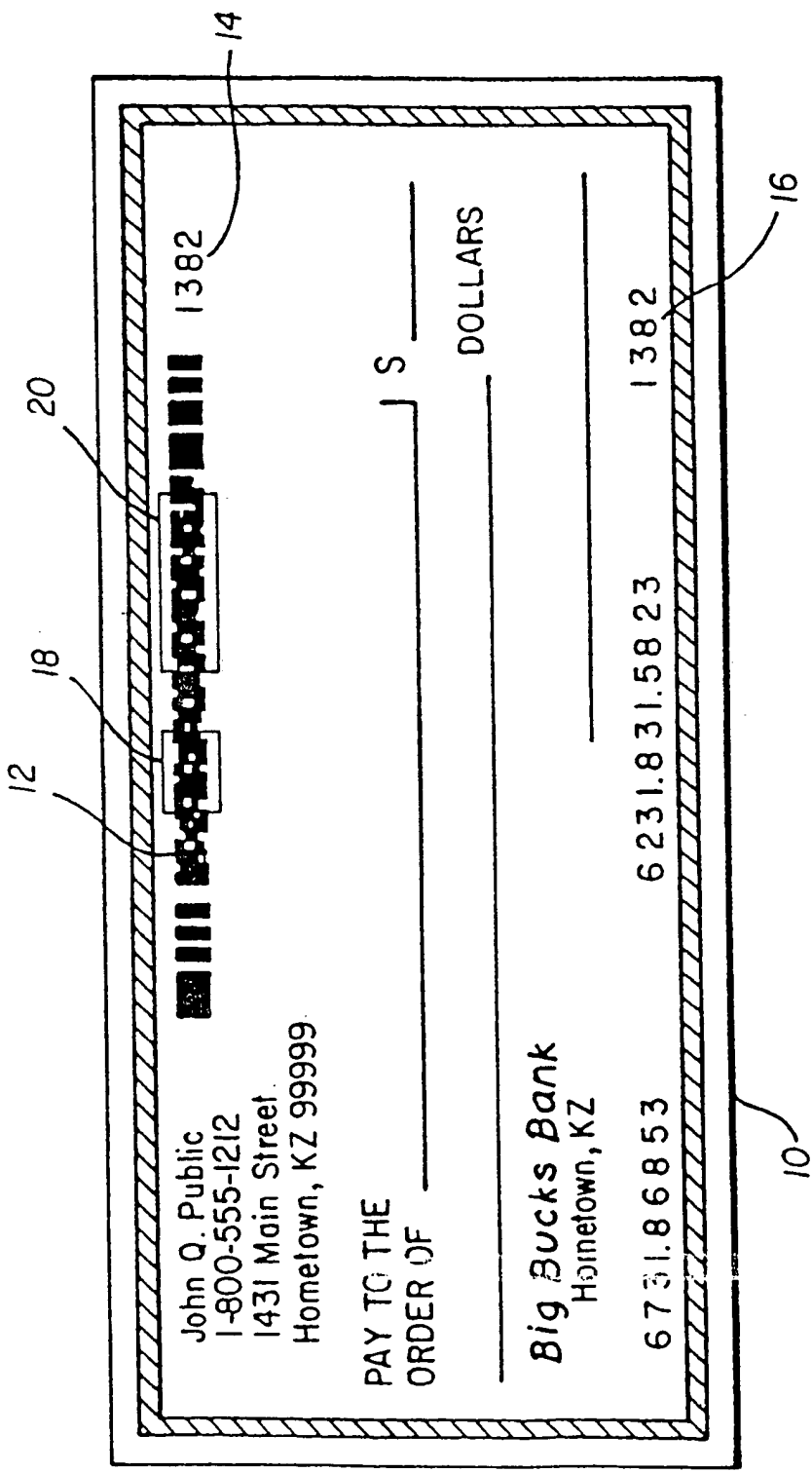


FIG. 1

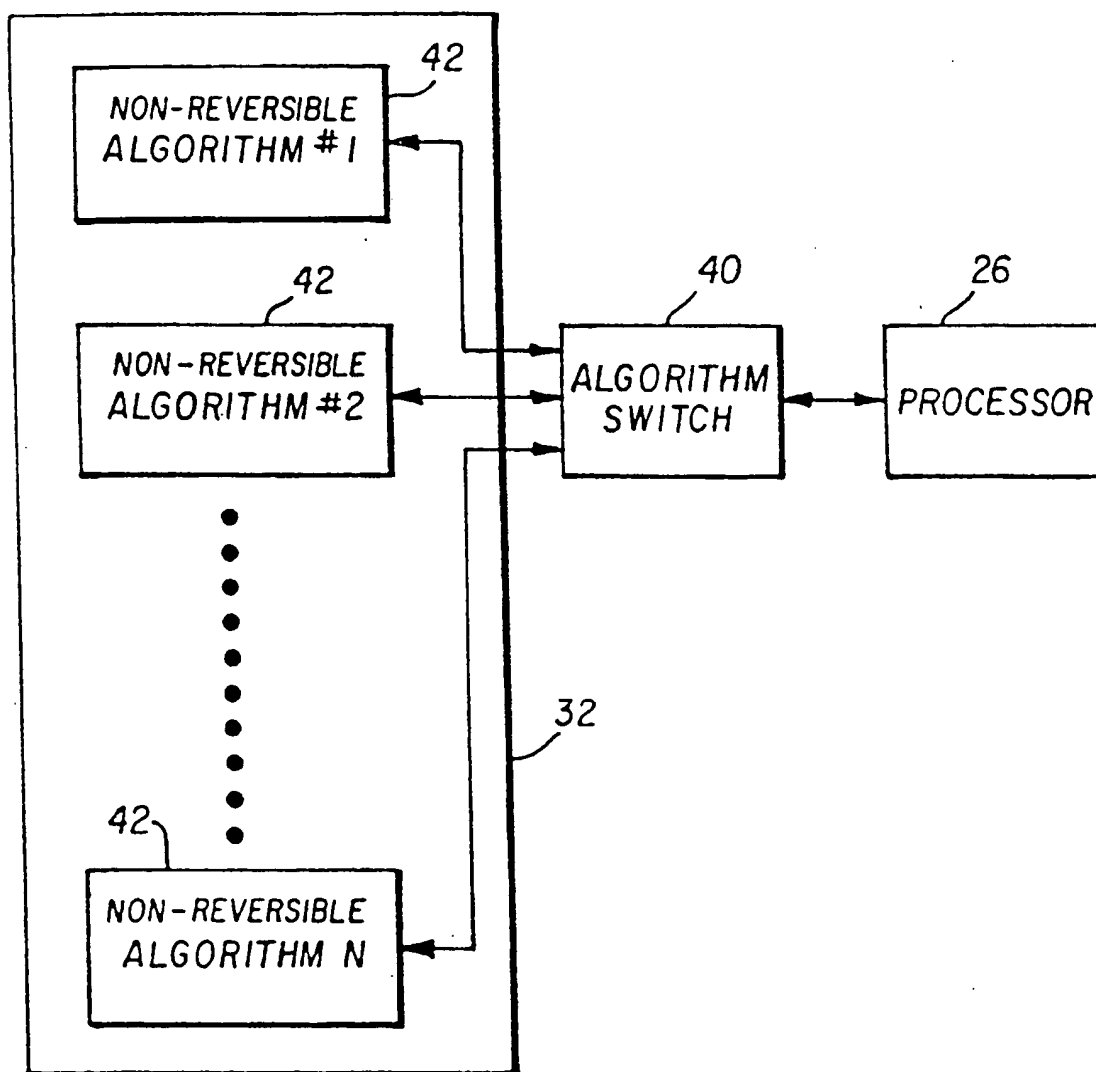


FIG. 3

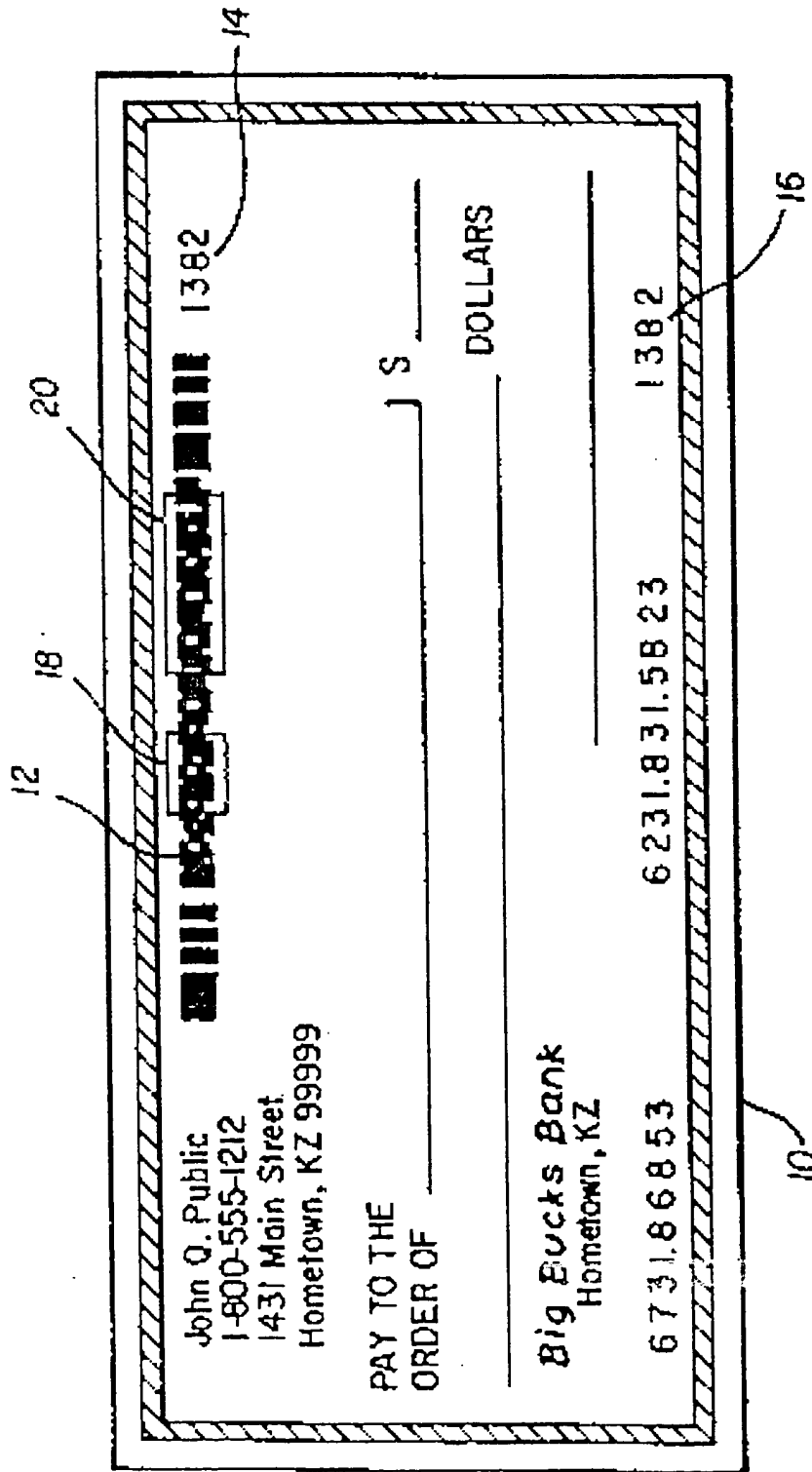


FIG. 1

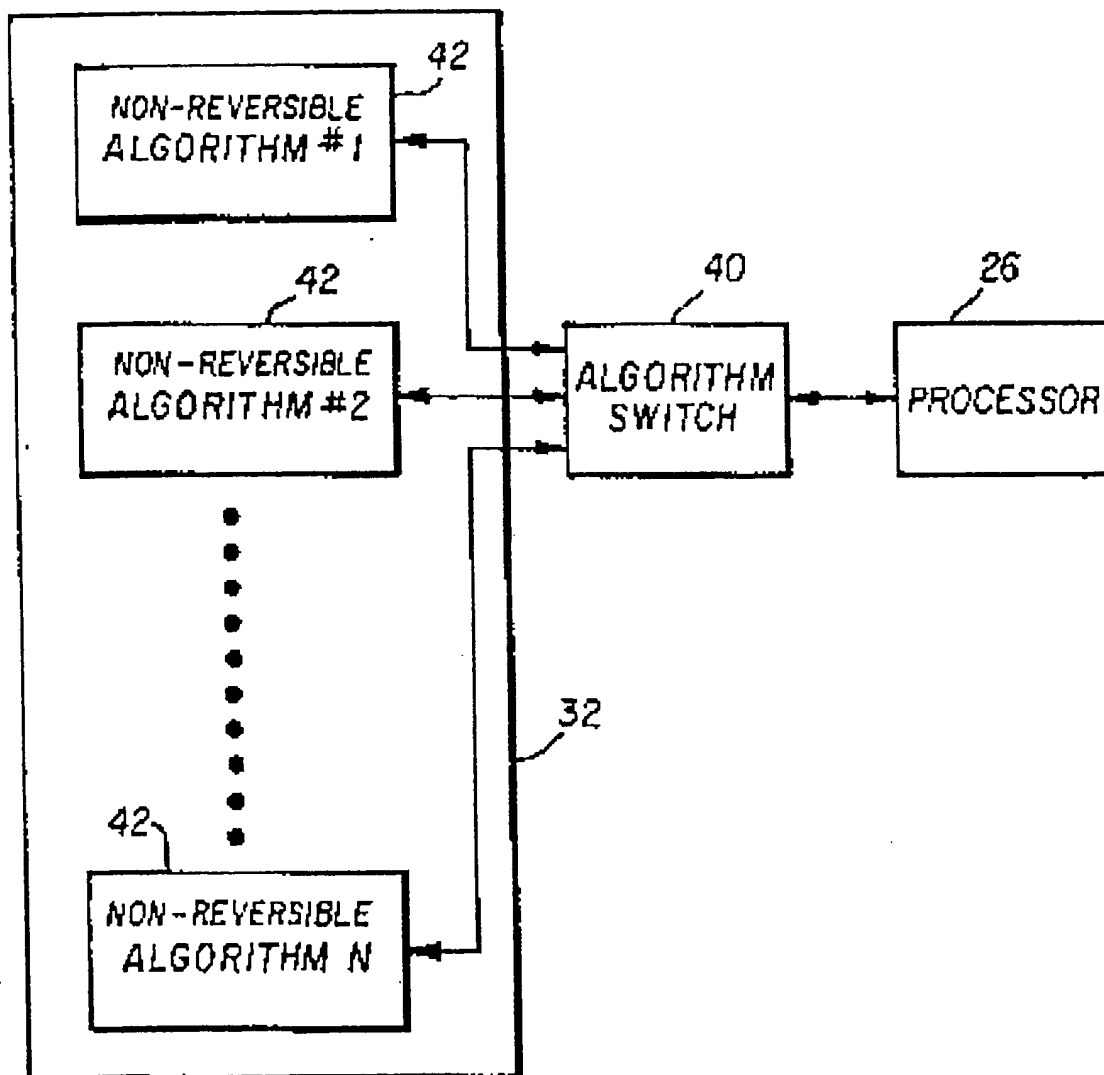


FIG. 3



**This Page is Inserted by IFW Indexing and Scanning  
Operations and is not part of the Official Record**

**BEST AVAILABLE IMAGES**

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ BLACK BORDERS
- ☐ IMAGE CUT OFF AT TOP, BOTTOM OR SIDES
- ☒ FADED TEXT OR DRAWING
- ☐ BLURRED OR ILLEGIBLE TEXT OR DRAWING
- ☐ SKEWED/SLANTED IMAGES
- ☐ COLOR OR BLACK AND WHITE PHOTOGRAPHS
- ☐ GRAY SCALE DOCUMENTS
- ☐ LINES OR MARKS ON ORIGINAL DOCUMENT
- ☐ REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY
- ☐ OTHER: \_\_\_\_\_

**IMAGES ARE BEST AVAILABLE COPY.**

**As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.**